# Esecurity: secure internet & e-passports, summer 2014
### Michael Nüsken

## 10. Exercise sheet
### Hand in solutions until Monday, 23 June 2014, 13:00

**Exercise 10.1** (Doc 9303). (14+4 points)

To answer the following questions read Doc 9303 and further reading, where required.

(i) What bit rates are possible for the communication between a MRTD and a reader? $\boxed{4}$

(ii) What is published in the ICAO PKD? Find the up to date CSCA certificate of Germany. For which time period is it valid and for which period is it used to sign? $\boxed{4}$

(iii) Imagine you work for a government, which wants to introduce the eMRTD. You are asked to decide which cryptographic scheme should be used in their Country Signing CA.

List all possible schemes. Which of them is the best? Why? Compare the runtime, the key size and the security of these schemes. $\boxed{6+3}$

(iv) In the lecure we saw "M / M" in the sex field of an Utopia visa. Find out what "M / M" stands for. What format does the sex field have? $\boxed{+1}$

**Exercise 10.2** (Entropy of the MRZ). (4 points)

Give a first rough upper bound on entropy of the MRZ by simply considering the types of entries for all involved places. Next reduce this bound using reasonable assumptions on the information. What else can you do using publicly available information of a given person? $\boxed{4}$